Aaron M. Sheanin (SBN 214472)
ASheanin@RobinsKaplan.com
Christine S. Yun Sauer (SBN 314307)
CYunSauer@RobinsKaplan.com
ROBINS KAPLAN LLP
46 Shattuck Square, Suite 22
Berkeley, CA 94040
Telephone: (650) 784-4040
Facsimile: (650) 784-4041

Attorneys for Plaintiffs and the Proposed Classes

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DEBORAH WESCH, DARIUS CLARK, JOHN H. COTTRELL, WILLIAM B. COTTRELL, RYAN HAMRE, GREG HERTIK, DAISY HODSON, DAVID LUMB, KYLA ROLLIER and JENNY SZETO, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

YODLEE, INC., a Delaware corporation, and ENVESTNET, INC., a Delaware corporation,

Defendants.

Civil Case No. 3:20-cv-05991-SK

OPPOSITION TO YODLEE, INC.'S MOTION TO DISMISS PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 12(b)(6)

Hearing Date: February 1, 2021
Hearing Time: 9:30 a.m.
Courtroom C – 15th Floor

Honorable Sallie Kim

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

STATEMENT OF THE ISSUES

Whether the Amended Complaint, drawing all reasonable inferences in the light most favorable to Plaintiffs, states a claim upon which relief can be granted under Federal Rule of Civil Procedure 12(b)(6). *See Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009).

I. INTRODUCTION

Defendants Yodlee, Inc. and Envestnet, Inc. are the largest aggregators of consumer financial data in the United States. They profit by selling access to individualized profiles that they construct for millions of Americans from highly sensitive financial data. The data needed to create and update these detailed financial profiles over time is the kind of information (e.g., current bank balances, transaction details, and credit card information) that individuals are loath to turn over. So, rather than ask Plaintiffs or Class members for their highly sensitive financial information directly, Defendants simply acquire that data by deceit.

The scheme is rather simple. FinTech Apps, like PayPal, use Defendants' software to connect their users' financial accounts to their App. Defendants exploit that relationship to acquire Plaintiffs' and Class members' login credentials, allowing them to connect and extract highly sensitive financial data directly from Plaintiffs' and Class members' banks on an ongoing basis, without ever asking for permission. Defendants deceive Plaintiffs and Class members into providing their login credentials by designing the process to appear as though it involves a secure connection to their home financial institutions. However, unbeknownst to Plaintiffs and Class members, they are not logging directly into their banks; they are typing their information into a Defendant-made portal that stores these credentials before using them to harvest data on every single transaction, payment, or charge that Plaintiffs and Class members make. Defendants continuously exploit these credentials to create a living financial profile on each Plaintiff and Class member, data that is worth millions of dollars. Plaintiffs and Class members never agreed to grant Defendants ongoing access to their accounts, or to systematically monitor the most minute and intimate details of their personal financial lives. Had they known the truth, they would never have used Yodlee.

Defendants' conduct, which has drawn the attention of members of Congress and is the subject of an ongoing investigation by the Federal Trade Commission, gives rise to each of Plaintiffs' claims for: (a) privacy violations under the common law and the California Constitution; (b) violations of federal law under the Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA"); (c) violations of California's Comprehensive Data

Access and Fraud Act ("CDAFA"), Anti-Phishing Act, and Unfair Competition Law ("UCL"); and (d) deceit and unjust enrichment.

Defendants' specific attacks on the various elements of these causes of action turn on either inapposite case law or a mischaracterization of Plaintiffs' allegations and have no merit. Nor can Yodlee escape liability by arguing that Plaintiffs consented to Defendants' collection, storage, and sale of their highly-sensitive data. While Plaintiffs may have let Defendants use their login credentials for the limited purpose of connecting their accounts to a FinTech App, any "consent" beyond that was ineffective, because it was procured by deceit. These allegations are more than sufficient to show that Defendants collected Plaintiffs' data without authorization, which harmed Plaintiffs by, among other things, causing them to lose valuable indemnity rights from their banks, placing them at risk of identity theft, and compromising the integrity of their data. The Court should deny Yodlee's motion to dismiss.

II. FACTUAL BACKGROUND

Although almost no one has heard of them, Defendants Yodlee and Envestnet compile and maintain highly detailed, personal financial profiles reflecting bank balances and transaction history, among other things, for millions of Americans. Defendants acquire this data by deceit, using software they provide to FinTech Apps to harvest Class members' financial institution login credentials. For example, when a user tries to connect one of their accounts to PayPal, Yodlee's software makes the connection. ¶ 55.[1] The user is presented with a screen that resembles the exact look and feel of the user's bank—i.e., same logo, color scheme, and font—and prompted to log in with their bank username and password, just as they would on the bank's website. ¶¶ 55-56. However, this is not a bank-run portal, but Yodlee's application programming interface ("API"). *Id*. Plaintiffs and Class members who enter their usernames and passwords on this screen are not interacting directly with their banks but instead providing their credentials to Defendants, which store them on their own servers for future use. ¶ 57.

[1] "¶ ___" refers to paragraphs of Plaintiffs' Amended Class Action Complaint, ECF No. 30. "MTD" refers to Yodlee, Inc.'s Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6), ECF No. 32. Capitalized terms not otherwise defined herein have the same meaning as in the Amended Complaint.

Although Paypal states that it "use[s] Yodlee to confirm your bank details and to check your balance and transaction as needed, which can help your PayPal payments go through," Yodlee itself never asks users for consent to access their bank data. ¶ 56. Nor does Yodlee disclose that, after acquiring users' banking credentials, Defendants continue to use them on an ongoing basis to harvest the most intimate details of their financial lives: every bill they paid to doctors and hospitals; every dollar they contributed to churches, synagogues, or charitable causes; and every purchase they made, no matter how private, including purchases that may reveal their political views, sexuality, or other intimate details of their lives. ¶¶ 11, 120. This can include years of historical transaction data, none of which is needed to connect that user's bank account to PayPal. ¶ 242. Other data that Defendants gather about those transactions include the applicable dates, times, locations, and counterparties for all transactions. ¶ 108. Defendants pull all this data onto their own servers to create a detailed profile for each Class member, designated by a "Yodlee-specific data identifier." MTD at 3; ¶¶ 108-09. Defendants continue to use Class members' bank credentials to update these profiles long after Yodlee linked their accounts to PayPal. ¶¶ 10, 58. This is true even if Class members never use PayPal again. *Id.*

But Defendants do not merely collect and store this data; they sell it. ¶ 4. Investment firms pay millions of dollars for annual subscriptions to the data Defendants have accumulated. ¶ 11. Defendants refer to these customers as "analytics and insights users." ¶ 116. Yet once Defendants sell this data, they exercise no control over what their customers do with it, and distribute the data in unencrypted plain text files. ¶¶ 13-15.

Alarmed by this misconduct, Senators Ron Wyden and Sherrod Brown and Congresswoman Anna Eshoo urged the FTC to open an investigation into Envestnet. ¶¶ 119-23. These members of Congress expressed concern that Envestnet "does not inform consumers that it is collecting and selling their personal financial data," given that the data they collect can reveal some of the most sensitive and intimate information about Plaintiffs' and Class members' lives. ¶ 120. These members of Congress rejected Envestnet's assurance that "consumers' privacy is protected because it anonymizes their personal financial data," since "for years researchers have been able to re-identify the individuals to whom the purportedly anonymized data belongs with

just three or four pieces of information." ¶¶ 119-23. In response, the FTC opened an investigation into Defendants, which remains ongoing. ¶ 123.

Organizations from all ends of the political spectrum also have warned about Defendants' practices, including the Consumer Financial Protection Bureau, the American Bankers' Association, and Jamie Dimon, CEO of JPMorgan Chase & Co. ¶¶ 87-93. Defendants' conduct harms Plaintiffs and Class members in various ways, including through loss of the protections they enjoy as long as their financial data remains in a secure banking environment, loss of control over their valuable property, and increased risk of identity theft and fraud. ¶¶ 97-99.

III. ARGUMENT

A. Legal Standard

On a Rule 12(b)(6) motion, the court must "accept as true all of the factual allegations contained in the complaint," *Erickson v. Pardus*, 551 U.S. 89, 94 (2007), and construe them "in the light most favorable to the [Plaintiffs]." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). A claim may be dismissed "only where there is no cognizable legal theory," or the complaint does not plead sufficient facts to "state a facially plausible claim to relief." *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010) (citations omitted). A claim is facially plausible when the facts alleged allow the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). As to Rule 9(b)—which Defendants contend applies to two of Plaintiffs' CFAA claims, as well as the claims for deceit and unjust enrichment—the pleading standard "requires only that the circumstances of fraud be stated with particularity." *United States v. Corinthian Colls.*, 655 F.3d 984, 992 (9th Cir. 2011). "Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally." Fed. R. Civ. P. 9(b). Further, allegations of omission-based fraud do not require the same level of specificity as those involving affirmative misstatements. *See MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1096 (N.D. Cal. 2014) ("[A] plaintiff alleging an omission-based fraud will not be able to specify the time, place, and specific content of an omission." (internal quotations and citations omitted)).

B. The Complaint States Plausible Claims for Violations of Common Law Intrusion Upon Seclusion and the California Constitution

In California, constitutional and common law privacy violations are so similar that "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Tracking*, 956 F.3d at 601 (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). Both issues present "mixed questions of law and fact"; the "highly offensive" inquiry, in particular, is "best left to a jury." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1059 (N.D. Cal. 2014) ("*Opperman I*") (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 39-40 (1994)); *see also id.* at 1061.

1. Plaintiffs Plead a Reasonable Expectation of Privacy in Their Data and the Profiles Defendants Create Based On That Data

Plaintiffs reasonably expected that Defendants would not continuously harvest and sell their financial data after connecting their bank accounts to PayPal. In *Facebook Tracking*, the Ninth Circuit reversed dismissal of allegations that Facebook violated users' privacy by improperly tracking their internet usage after they had logged out of the social network. 956 F.3d at 602. The Court considered several factors in reaching that conclusion. Each weighs in favor of finding that Plaintiffs here have a reasonable expectation of privacy in their data. *Id.* at 603.

Amount and extent of data collected: Plaintiffs' claims are supported by the "enormous amount[s] of individualized data" Defendants collected about them. *Id.* Defendants' argument that Plaintiffs have no reasonable expectation of privacy in the details of any particular transaction because "the merchant who made the sale," or a bystander, might see that information, MTD at 6-7, is a straw man. Defendants did not incidentally stumble upon data for a single transaction; they deliberately invaded Plaintiffs' privacy to gather highly sensitive location, date, time, amount, and counterparty data on *thousands* of transactions.

Nature of the data collected: Defendants collect "financial records" about Plaintiffs that contain "the most intimate details of [their] lives" and thus are "expected to be kept private." *See United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013).[2] This data can "reveal

[2] Plaintiffs' reasonable expectation of privacy is further supported by multiple state and federal

information" about a person's "health, sexuality, religion, political views, and many other personal details." ¶ 120. It is far more sensitive than the internet browsing or television-watching histories in which courts have repeatedly found people have a reasonable expectation of privacy. *See Facebook Tracking*, 956 F.3d at 603; *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017).

The manner in which Defendants collect the data: Deceptive conduct is a "plus factor that is significant in establishing an expectation of privacy." *Heeger v. Facebook*, No. 18-CV-06399-JD, 2019 WL 7282477 at *4 (N.D. Cal. Dec. 27, 2019) (quotations and citations omitted). Plaintiffs allege that Defendants: (1) failed to disclose that Yodlee would harvest far more data than "needed" to facilitate financial transactions, and (2) induced Plaintiffs to enter login credentials into an interface deceptively disguised to resemble those of their banks. ¶¶ 55-57. Defendants' ongoing abuse of Plaintiffs' credentials long *after* Yodlee linked their accounts to PayPal confirms the plausibility of Plaintiffs' claim. *Facebook Tracking*, 956 F.3d at 604-06 (plaintiffs had a reasonable expectation that Facebook would not track users after logging out).

Tellingly, Defendants do not dispute Plaintiffs' reasonable expectation of privacy in their data and instead argue that this expectation dissipates once Class members' names are replaced with a Yodlee-specific identifier and aggregated with other information. MTD at 3, 5-7. But Defendants' attempts to anonymize Plaintiffs' highly sensitive financial data *after the fact* do not address the intrusion upon seclusion caused each time Defendants *collect* Plaintiffs' data without authorization. *Hernandez*, 47 Cal. 4th at 286 (explaining that intrusion upon seclusion occurs when "the defendant . . . intentionally intrude[s] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. . . ."). Moreover, courts in this district recognize that "[i]nformation need not be personally identifying to be private," rejecting "anonymization" as a defense to invasion of privacy claims.[3] *In re Google Referrer Header*

laws, which enshrine a right to financial privacy and impose restrictions on the government's and financial institutions' treatment of consumers' private financial data. ¶¶ 70-86.

[3] Worse, the data Defendants sell is not truly anonymous, as it takes just three or four pieces of additional information to *reidentify* Class members. ¶ 112.

Privacy Litig., 465 F. Supp. 3d 999, 1009–10 (N.D. Cal. 2020), *motion to certify appeal denied*, No. 10-CV-04809-EJD, 2020 WL 5545155 (N.D. Cal. Sept. 16, 2020); *Vizio*, 238 F. Supp. 3d at 1233 (finding plaintiffs' expectation of privacy in anonymized television-viewing histories reasonable). This Court should reach the same conclusion here, where Plaintiffs' allegations that Defendants "compiled highly personalized profiles" of consumers' "sensitive . . . histories and habits . . . prevent [the court] from concluding that the Plaintiffs have no reasonable expectation of privacy." *Facebook Tracking*, 956 F.3d at 604 (footnote omitted).

Valley Bank v. Superior Court, 15 Cal. 3d 652 (1975), does not support Defendants' argument that they may do as they wish with Class members' sensitive personal data as long as they replace Class members' names with Yodlee-specific identifiers.[4] MTD at 6. In *Valley Bank*, the California Supreme Court reversed a trial court order requiring disclosure of confidential customer financial information pursuant to a subpoena. *Id.* at 657-58. Critical to this case, the court noted the need to protect "the right of bank customers to maintain reasonable privacy regarding their financial affairs." *Id.* at 657. Ignoring that rationale, Defendants cherry pick dicta in which the court finds the "deletion of the customer's name" to be "inappropriate in the instant case," where the identity of the bank's customers was relevant to show its alleged relationship with the Teamsters Union. *Id.* at 658. The Court should reject Defendants' argument.[5]

2. Defendants' Invasion of Privacy is Highly Offensive

"Actionable invasions of privacy . . . must be 'highly offensive' to a reasonable person, and 'sufficiently serious' and unwarranted so as to constitute an 'egregious breach of the social norms.'" *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 295). Even

[4] Defendants also claim that they fall within a California Consumer Privacy Act ("CCPA") exemption for sale of "aggregated, anonymized transactional data." MTD at 7. Plaintiffs have not brought a claim for violation of the CCPA, so this point is irrelevant. *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), does not support Defendants' contention that their conduct is "routine commercial behavior." MTD at 7. *Folgelstrom* did not involve a sweeping ploy to harvest data and banking credentials from millions of Americans; it involved collection of customers' zip codes so defendant could mail them coupons. 195 Cal. App. 4th at 992.

[5] *Valley Bank* is also more than 45 years old. Because "[a]dvances in technology can increase the potential for unreasonable intrusions into personal privacy," this decision should have no bearing on this case. *Facebook Tracking*, 956 F.3d at 599; *see also McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019) ("Current privacy expectations are developing, to say the least.").

routine data collection practices may be highly offensive when conducted deceptively. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 150-51 (3d Cir. 2015) ("Characterized by deceit and disregard, the alleged conduct raises different issues than tracking or disclosure alone. . . . [U]sers . . . are entitled to rely on the public promises of the companies they deal with.") (applying California law); *McDonald*, 385 F. Supp. 3d at 1035 (plaintiff sufficiently pled "highly offensive conduct" through allegations that defendant secretly harvested users' personal information to generate unique profiles of users).

Defendants' deceptive collection of Class members' financial data violates social norms. ¶¶ 102, 143, 240, 242. Defendants misrepresented that they were merely collecting data "as needed" to make PayPal function when in fact, they were taking Plaintiffs' banking credentials to continue gathering their sensitive data long after Yodlee linked their accounts. ¶¶ 10, 58. This invasion of privacy is highly offensive. *See Facebook Tracking*, 956 F.3d at 603 ("Plaintiffs' allegations of surreptitious data collection when individuals were not using Facebook . . . could highly offend a reasonable individual."); *McDonald*, 385 F. Supp. 3d. at 1035 (allegations that "defendants surreptitiously gathered user-specific information [and] continue to gather information and track individual users" sufficient).

Defendants are wrong to argue that conduct is only highly offensive when it involves "gruesome photographs" or the disclosure of a plaintiff's medical records. MTD at 7. Courts consistently find far less serious conduct to be highly offensive, including the collection of anonymized TV viewer data, *see Vizio*, 238 F. Supp. 3d at 1233, or the use of "cookies" to track users online, *see Google Cookie*, 806 F.3d at 151. Plaintiffs' allegations clear that bar.

Defendants' aggregation and anonymization of data before selling it to third parties does not make the collection of it any less offensive. Defendants also fail to identify any authority providing that Plaintiffs' claim survives only if someone *successfully* de-anonymized their data.[6]

[6] Defendants cite *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012), where the less expansive collection of less sensitive LinkedIn browsing histories was nowhere near as offensive as Defendants' conduct here. *Low* also is distinguishable in that it involved tracking users while they were using the app—not for years afterwards. *See Facebook Tracking*, 956 F.3d at 606 n.8 (distinguishing *Low*). *Moreno v. Bay Area Rapid Transit District*, No. 17-02911, 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017), is also inapposite because it turned on plaintiffs' failure

To the contrary, the "*likelihood* of serious harm" shows that the intrusion was highly offensive. *Facebook Tracking*, 956 F.3d at 606 (emphasis added).

C. Plaintiffs State a Claim Under California's Comprehensive Data Access and Fraud Act ("CDAFA")

Defendants alleged misconduct violated at least six provisions of the CDAFA (sometimes referred to as "Section 502"). Those provisions share two common elements: (1) that Defendants' "knowingly accessed" data, a computer, a computer system or a computer network and (2) took some action with regard to that data or computer "without permission." ¶¶ 205-10.[7] For instance, a defendant violates Section 502(c)(2) when it "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Defendants do not dispute that they knowingly accessed Plaintiffs' data and their financial institutions' computers, or that they took, copied, and made use of Plaintiffs' data. Nor do they meaningfully challenge any of the elements of the other CDAFA provisions under which Plaintiffs assert claims. Instead, Defendants take the unsupported positions (1) that Plaintiffs may not assert a CDAFA claim at all, or (2) that the consent Plaintiffs supposedly granted gave Defendants license to collect whatever data Defendants wanted, whenever they wanted, and do with it as they pleased. These arguments fail.

1. Plaintiffs Have Standing to Bring CDAFA Claims.

Plaintiffs may enforce their rights under the CDAFA because they "suffer[ed] damage or loss by reason" of Defendants' violations of the statute. Cal. Penal Code § 502(e). As Defendants admit, "the CDAFA does not set a minimum threshold" for damage or loss. MTD at 12. *NovelPoster v. Javitch Canfield Grp.,* 140 F. Supp. 3d 954, 964 (N.D. Cal. 2014).

Plaintiffs sufficiently allege that Defendants caused them a "loss." In *Facebook Tracking*, the Ninth Circuit reversed dismissal of a CDAFA claim on precisely this issue. 956 F.3d at 600.

---

to allege that defendant was "aware of the data collection." *Id.* at *8. Here, Plaintiffs allege that Defendants collected Plaintiffs' data willfully.

[7] Cal. Pen. §§ 502(c)(3) and 502(c)(6) do not contain access requirements, but rather require that defendants took certain actions both knowingly and without permission.

The Court found that Plaintiffs alleged a loss under the statute because, among other things, they "sufficiently allege that Facebook profited from [their] valuable data," plaintiffs "did not provide authorization for the use of their personal information," and plaintiffs did not "have any control over" Facebook's use of that data "to produce revenue." *Id.* at 600-01. Here, too, Plaintiffs allege that Defendants collected and profited from their data without permission. That suffices.

Plaintiffs allege that Defendants caused them to suffer damage including costs associated with: (1) the loss of control over valuable property, *i.e.*, their highly sensitive personal data; (2) increased risk of identity theft; and (3) loss of valuable indemnification rights provided through Plaintiffs' and Class members' financial institutions. ¶¶ 97-99. These allegations both confer standing and establish the damage component of those CDAFA provisions that contain one. *See* Cal. Pen. Code §§ 502(c)(1), 502(c)(4).[8]

2. Defendants Accessed Plaintiffs' Accounts "Without Permission"

The CDAFA "only requires *knowing* access, not *unauthorized* access" to Plaintiffs' data. *Henry Schein, Inc. v. Cook*, No. 16-CV-03166-JST, 2017 WL 783617, at *5 (N.D. Cal. Mar. 1, 2017) (emphasis added) (citing *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015)). A combination of *knowing access* and *unauthorized use* will violate the statute: "using valid login credentials and subsequently misusing the information obtained constitutes a section 502[(c)(2)] violation." *Id.*; *Christensen*, 828 F.3d at 790 (finding that term "access" in CDAFA extends to "logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly"); *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 454 (N.D. Cal. 2018) (denying motion to dismiss CDAFA claim where plaintiffs' consent did not extend to defendant's battery throttling). That is exactly what Plaintiffs allege here: Defendants knowingly used Plaintiffs' and Class members' login credentials to harvest highly sensitive personal data, and misused that information for Defendants' own gain.

[8] Notably, a defendant violates Cal. Pen. Code §§ 502(c)(1) if it "damages" *or* "otherwise uses any data." Regardless of Plaintiffs' allegations of damage, there is no dispute that Defendants *used* Plaintiffs' highly sensitive personal data and credentials.

Defendants make the outlandish suggestion that as long as Plaintiffs granted Defendants access to their highly sensitive data "for any purpose," they granted access to their data for *every* purpose. MTD at 14. Such a rule would be contrary to law. Even if Defendants had valid access to Plaintiffs' and Class members' login credentials—and they did not, because any consent Plaintiffs granted was ineffective; *see infra* § III.E.2—Defendants' subsequent misuse of the data violates Section 502. *Henry Schein*, 2017 WL 783617, at *5.[9]

D. Plaintiffs State a Claim for Violation of the Stored Communications Act

The SCA "codif[ies] a substantive right to privacy," *Facebook Tracking*, 956 F.3d at 598 (citation omitted), recognizing that individuals "have a legitimate interest in the confidentiality of communications in electronic storage." *Google Referrer Header*, 465 F. Supp. 3d at 1009 (citations omitted). The SCA requires that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Defendants' conduct violates 18 U.S.C. § 2702[10] and the SCA.[11]

[9] Defendants' argument that Plaintiffs must allege "circumvent[ion of] technical or code-based barriers," MTD at 15 n.5, relies on outdated law. Courts now agree that "section 502 does not require that defendant "overcome code-based barriers for [it] to be potentially liable for the unauthorized taking or destruction of [plaintiff's] data." *Erhart v. BofI Holding, Inc.*, 387 F. Supp. 3d 1046, 1057 (S.D. Cal. 2019); *Pierry, Inc. v. Thirty-One Gifts, LLC*, No. 17-CV-03074-MEJ, 2017 WL 4236934, at *7 (N.D. Cal. Sept. 25, 2017).

[10] Plaintiffs' claim for violation of the SCA contains a scrivener's error, referring to 18 U.S.C. § 2701 (prohibiting unauthorized *access*) rather than § 2702 (prohibiting unauthorized *disclosure*). ¶¶ 155-67. Regardless, the allegations also support a § 2701 violation—namely, that Defendants (1) intentionally accessed without authorization, or in excess of authorization, "a facility through which an electronic communication service is provided" and (2) thereby obtained access to electronic communications (3) while it was in electronic storage in such system. § 2701(a)(1). The relevant "facilities" are the servers and computer systems of the financial institutions that maintained Plaintiffs' and Class members' data. ¶¶ 8, 10. The data are "communications." *See infra* § III.D.2. Defendants accessed such communications without or in excess of authorization for the same reasons described with regard to the CFAA claim. *See infra* §§ III.E.2, 3. Plaintiffs reserve the right to amend their complaint to assert a § 2701 claim.

[11] Defendants do not—and cannot—dispute Plaintiffs' plausible allegations that Defendants "knowingly divulge" Plaintiffs' data to third parties by selling this sensitive banking data. ¶¶ 2, 4, 46, 52, 54, 170.

1. Yodlee Is an "Electronic Communication Service" Provider

Courts broadly construe the definition of an electronic communication service ("ECS") provider under the SCA. The statute defines an ECS provider as "*any* service which provides users thereof the ability to send or receive . . . electronic communications." *Crispin v. Christian Audigier, Inc*., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (quoting 18 U.S.C. § 2510(15)) (emphasis in opinion). Courts interpret the definition to include a wide range of services, including where communication is not its primary function. *See, e.g.*, *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (ECS definition included airline that provided travel agents with a computerized travel reservation system with a messaging function).

Yodlee is an ECS provider. It provides Plaintiffs, FinTech Apps and financial institutions the ability to send and receive electronic communications, namely consumer data and credentials. ¶¶ 7, 55-57, 162. Defendants' reliance on the unpublished decision in *Casillas v. Cypress Ins. Co*., 770 F. App'x 329, 331 (9th Cir. 2019), is misplaced. MTD at 9. There, the Ninth Circuit concluded that a system enabling document uploads and downloads did not qualify as an ECS provider because it did not allow direct communication. By contrast, here, Defendants do allow Plaintiffs, banks and FinTech Apps to communicate directly. ¶¶ 7, 56, 162.

2. The Data Defendants Collect, Store and Divulge Are the "Contents" of Users' "Communications"

The "contents of a communication" may include "any information concerning the substance, purport, or meaning of that communication." *Xie v. Lai*, No. 19-MC-80287-SVK, 2019 WL 7020340, at *5 (N.D. Cal. Dec. 20, 2019) (citation omitted). Courts distinguish content from "record information," such as the "to/from" fields of an email or a phone number, which do not disclose any substance. *See United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008). This determination is case-specific. *See Google Cookie*, 806 F.3d at 137 ("[T]he line between contents and metadata is . . . contextual with respect to each communication."); *Rainsy v. Facebook, Inc.*, 311 F. Supp. 3d 1101, 1114–15 (N.D. Cal. 2018) (holding that "liking" a page on Facebook constitutes "'content' as information concerning the meaning of a communication").

Here, the sensitive financial data Defendants unlawfully collected, stored, and sold are content protected by the SCA because they reveal substance—what the Plaintiffs bought, from whom, when, and where. This is "much more information about [their] activity" than could be obtained from "record information," like a phone number. *Forrester*, 512 F.3d at 510 n.6.[12]

3. Defendants Keep Plaintiffs' Data in "Electronic Storage"

The SCA defines "electronic storage" as *either* "temporary, intermediate storage" of communications "incidental to the electronic transmission thereof" *or* storage of such communications "for purposes of backup protection." 18 U.S.C. § 2510(17); *see Crispin*, 717 F. Supp. 2d at 982–83. Courts have held that the term "electronic storage" should be "broadly construed, and not limited to particular mediums, forms, or locations." *Facebook Tracking*, 956 F.3d at 609 (citations omitted).

Defendants do not dispute that they maintain years of highly sensitive financial data in a personal profile for each Plaintiff and Class member for sale to third parties. ¶¶ 4, 46, 164.[13] Rather, they argue that they do not "store" the data because they hoard it indefinitely. MTD at 11. This is just wrong. Communications "reserved for future use"—like Defendants' sales to third parties—are maintained in electronic storage. *See Hately v. Watts*, 917 F.3d 770, 786 (4th Cir. 2019); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). Any other interpretation would be absurd, granting immunity from the SCA so long as the violators keep users' sensitive data and do not dispose of it.

For all of the reasons stated above, Plaintiffs plausibly state a claim under the SCA.

---

[12] Defendants' authorities are readily distinguishable. In *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1102, 1105 (9th Cir. 2014), the content at issue involved "HTTP referrer information" disclosed by Facebook to third parties after a user clicked on an advertisement. *Chevron Corp. v. Donziger*, No. 12-mc-80237 CRB (NC), 2013 WL 4536808, at *2 (N.D. Cal. Aug. 22, 2013), involved the disclosure of users' names, phone numbers, and other information incidental to the creation of each user's email address. *In re Application for the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 121 (E.D. Va. 2011), and *Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1195 (S.D. Iowa 2000), did not involve the details of users' purchases such as the location, date, time, amount, subject, and counterparty.

[13] In both *In re Toys R Us, Inc. Priv. Litig.*, No. 00-CV-2746, 2012 WL 34517252, at *3 (N.D. Cal. Oct. 9, 2001) and *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1059 (N.D. Cal. 2012), the data at issue was on users' devices. *See* MTD at 11. Here, Defendants maintain Plaintiffs' data in their own storage.

E. Plaintiffs State a Claim Under the Computer Fraud and Abuse Act ("CFAA")

Plaintiffs allege that Defendants violated the CFAA in at least four ways:

1. by intentionally accessing "protected computers" without authorization or in excess of authorization, and thereby obtaining information contained in financial records (18 U.S.C. § 1030(a)(2)(A), (C); ¶¶ 220-21);

2. by knowingly accessing a protected computer without authorization or in excess of authorization and, with intent to defraud, furthering a scheme to "obtain anything of value" (18 U.S.C. § 1030(a)(4); ¶¶ 222-24);

3. by knowingly transmitting information in order to intentionally cause damage to a protected computer (18 U.S.C. § 1030(a)(5)(B), (C); ¶¶ 227-28); and

4. by knowingly and with the intent to defraud trafficking in computer passwords (18 U.S.C. § 1030(a)(6); ¶¶ 229-30).

The Amended Complaint plausibly alleges each violation. Plaintiffs repeatedly allege that Defendants acted with intent to access their financial institutions' computers, which are "protected computers" under the statute;[14] that Defendants acted without, or in excess of, authorization, *see infra* § III.E.2, 3; that Defendants intended to and did cause damage to protected computers, *see infra* § III.E.4; that Defendants acted with intent to defraud, *see infra* § III.E.5; and that Defendants trafficked in Plaintiffs' banking passwords, *see infra* § III.E.6. Unlike the cases that Defendants cite, these allegations far exceed a bare recitation of the elements of a CFAA claim. MTD at 13 (citing *Gonzales v. Uber Techs., Inc*., 305 F. Supp. 3d 1078, 1090 (N.D. Cal. 2018); *Brodsky v. Apple, Inc*., No. 19-CV-00712-LHK, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019)). There is no need to "guess" how Defendants deceived Plaintiffs, *see* MTD at 13; the Amended Complaint describes it exactly. ¶ 67; *cf. Gonzales*, 305 F. Supp. 3d at 1090.

1. Plaintiffs Have Standing to Assert Violations of the CFAA

To assert a private right of action under the CFAA, a plaintiff must show a "loss to 1 or more persons . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). The

[14] The CFAA defines a "protected computer" to include the computer systems, data storage facilities, or communications facilities used by financial institutions or otherwise used in or affecting interstate or foreign commerce. 18 U.S.C. § 1030(e)(2)(A), (B).

CFAA defines the term "loss" broadly to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Courts in the Ninth Circuit "do not read 'loss' so narrowly," accepting time spent and costs "responding to an offense" as a "loss" under the statute. *See Ticketmaster LLC v. Prestige*, 315 F. Supp. 3d 1147, 1172-73 (C.D. Cal. 2018); *Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058, 1066 (9th Cir. 2016) ("*Power Ventures*") (holding that hours spent "analyzing, investigation, and responding" to unauthorized access constitute "loss" and provide a basis for a civil action under the CFAA); *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980 (N.D. Cal. 2008) (time spent analyzing what information was accessed sufficed); *United States v. Janosko*, 642 F.3d 40, 42 (1st Cir. 2011) (monitoring credit records sufficed).

Plaintiffs allege losses sufficient to exercise their private right of action under the CFAA for the same reasons as their CDAFA claim. *See* § III.C. *supra*.[15] As Defendants' data collection practices affected millions of individuals, these losses easily surpass the CFAA's $5,000 threshold. ¶ 132; *see In re Apple & AT&TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (aggregating individual damages).[16]

2. Defendants Took Plaintiffs' Data Without Authorization

Defendants are wrong to assert that Plaintiffs authorized gross invasions of their privacy. "Consent is only effective if the person alleging harm consented to 'the particular conduct, or to

[15] As discussed below, Defendants' deprived Plaintiffs of the indemnity rights to which they would otherwise be entitled from their financial institutions, which is a deprivation of a "property right." *See infra* §III.G.1; ¶¶ 92, 97; *see Singer Co. v. Superior Court*, 179 Cal. App. 3d 875, 890 (1986); *Beltran v. United States*, 441 F.2d 954, 960-61 (7th Cir. 1971).

[16] Defendants' remaining authorities are inapposite as they involve purely conclusory allegations or simple recitations of the threshold required for private plaintiffs to bring an action. *In re Google Android Consumer Priv. Litig.*, No. 11-MD-02264 JSW, 2013 WL 1283236, at *7 (N.D. Cal. Mar. 26, 2013) (setting forth "only a bare legal conclusion," couched as fact, that they incurred costs); *AtPac, Inc. v. Aptitude Sols., Inc.*, 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010) (only "conclusory allegations that plaintiff ha[d] been damaged and that it ha[d] suffered immediate and irreparable harm"); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 949 (N.D. Cal. 2014) (same); *Delacruz v. State Bar of California*, No. 16-cv-06858-BLF, 2018 WL 3077750, at *8 (N.D. Cal. Mar. 12, 2018) (same).

substantially the same conduct' [as that alleged] and if the alleged tortfeasor did not exceed the scope of that consent." *In re Google Location History Litig.*, 428 F. Supp. 3d 185, 190 (N.D. Cal. 2019) (quoting *Opperman v. Path, Inc.* 205 F. Supp. 3d 1064, 1072 (N.D. Cal 2016) ("*Opperman II*")); *see also In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 789–90, 792 (N.D. Cal. 2019) (users did not consent where disclosure "does not come close to disclosing the massive information-sharing program with business partners that the plaintiffs allege in the complaint"); *Apple & AT&TM Antitrust*, 596 F. Supp. 2d at 1308 (users who voluntarily downloaded software did not authorize phone throttling); *see also Harris v. Comscore, Inc.*, 292 F.R.D. 579 (N.D. Ill. 2013) (certifying CFAA class when defendant exceeded the scope of its consent by "intercepting user names, passwords, bank account numbers, credit card numbers, and other demographic information" and "selling the data collected").

As members of Congress have explained, Envestnet "does not inform consumers that it is collecting and selling their personal financial data." ¶ 122. The fact that Envestnet "asks its partners," like PayPal, to disclose this information "is not sufficient protection for users," because "Envestnet does not appear to take any steps to ensure that its partners actually provide consumers with such notice." *Id.*

Defendants' consent argument lacks merit. *First*, although Defendants contend that the disclosure in the PayPal app was sufficient to establish Plaintiffs' consent to Defendants' data practices, that disclosure said nothing of *Defendants' conduct*, only that Paypal would "check [users'] balance and transactions as needed" to "help [users'] Paypal payments go through." ¶ 56. That disclosure is woefully inadequate, given that Defendants copy Plaintiffs' bank login credentials and build a personal profile of every Class member, which is updated on an ongoing basis. Defendants' conduct bears no relation to the functionality of the PayPal app. Any consent a Plaintiff gave was not informed and thus not effective.

Second, Defendants are wrong to suggest that Plaintiffs consented to their data collection practices by entering their usernames and passwords into the Yodlee API. MTD at 18. Here, too, any consent was ineffective because it was based on deceit: Defendants' intentional design of the Yodlee interface to masquerade as Plaintiffs' banks. ¶¶ 57, 67.

Defendants' cases are off-point. They involve situations where the defendant indisputably had permission to access plaintiffs' systems. For example, in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the court dismissed CFAA claims that an employer brought against an employee based on alleged unauthorized access to a company computer, because it was undisputed that employee had rightful access to that machine. *Id*. at 1133; *see also Power Ventures*, 844 F.3d at 1066-67 (explaining that in *LVRC Holdings LLC* if "the employee accessed company computers without express permission, he would have violated the CFAA").

3. Defendants Exceeded Authorized Access

In any event, Defendants exceeded whatever authorization to access Plaintiffs' data they may have obtained. A defendant "exceeds authorization" by taking confidential information it is "not entitled to access, obtain, or transmit." *Synopsys, Inc. v. Ubiquiti Networks, Inc*., 313 F. Supp. 3d 1056, 1070 (N.D. Cal. 2018); *see Flextronics Int'l, Ltd. v. Parametric Tech. Corp*., 2014 WL 2213910, at *3 (N.D. Cal. May 28, 2014) (where defendant "concealed certain embedded technology" designed to collect data about plaintiff in software that plaintiff voluntarily used, defendant exceeded authorization). This is exactly what Plaintiffs allege here.[17]

Defendants misconstrue Plaintiffs' claim by suggesting that it turns solely on Defendants' subsequent *misuse* of data (though Defendants did that, too). MTD at 15. In fact, Plaintiffs allege that Defendants' access—which extended far beyond what was "needed" to enable PayPal to function—was excessive itself. ¶¶ 205-06, 220-21.

4. Plaintiffs Sufficiently Plead the "Damage" Defendants Caused

Plaintiffs sufficiently allege that Defendants caused them damage for purposes of 18 U.S.C. § 1030(a)(5)(A). The statute defines "damage" broadly to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "[I]t is not necessary for data to be physically changed or erased to constitute damage to that data." *Satmodo, LLC v. Whenever Commc'ns., LLC*, No. 17-0192, 2017 WL 6327132, at *3 (S.D. Cal. Dec. 8, 2017) (quotations omitted). "[A]lleged unauthorized access to [a computer system]

[17] Even under Defendants' own articulation of the rule, Plaintiffs allege "unauthorized procurement" of their data. MTD at 15.

and the disclosure of its information may constitute an impairment to the integrity of data even though no data was physically changed or erased." *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 996-97 (E.D. Cal. 2007) (citation and internal quotation marks omitted).

Here, Defendants impaired the integrity of Plaintiffs' data by: (1) accessing their data without authorization, ¶¶ 53-57; (2) using that unauthorized access to copy or remove the data from the secure banking environment, ¶¶ 93, 95-96; and (3) selling it without adequate controls over what purchasers do with it, including circulating the data in unencrypted plain text, ¶¶ 13, 118. Defendants have done far more damage than mere "economic harm due to the commercial value of the data itself." MTD at 16 (citing *NetApp, Inc. v. Nimble Storage, Inc*., 41 F. Supp. 3d 816, 834 (N.D. Cal. 2014)). Stealing passwords, like Defendants did here, "*necessarily compromises the security of a computer system and increases the risk of further damage*, because it enables hackers to later access password-protected computer systems, information, and data." *See NetApp, Inc. v. Nimble Storage, Inc.*, No. 5:13-cv-05058-LHK (HRL), 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) (citing S. Rep. No. 104-357, at 11 (1996)) (emphasis added). That harm is enough to state a CFAA claim.

5. Plaintiffs Allege Defendants' Intent to Defraud

Plaintiffs sufficiently allege that Defendants knowingly and "with intent to defraud" accessed a protected computer, as required by 18 U.S.C. §§ 1030(a)(4) and 1030(a)(6). Courts in this Circuit interpret "intent to defraud" to mean "unlawful access" or "wrongdoing." *See eBay Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (allegations that "defendant participated in dishonest methods to obtain the plaintiff's secret information" suffice). Plaintiffs allege that Defendants acted with intent to defraud through their "scheme to deceive Plaintiffs and Class members into thinking that they were providing their banking credentials directly to their bank, when in fact they were providing those credentials to Defendants." ¶ 224. This easily satisfies even the heightened pleading standard of Rule 9(b), explaining that Defendants (who) accomplished their fraudulent scheme by posing as Plaintiffs' financial institutions (how), when they linked their bank account to a third-party app (when and

where), deceiving them into turning over their bank log-in credentials and related data (what). ¶¶ 45, 55-57. No additional details are required.

6. Defendants Trafficked in Plaintiffs' Passwords

A person violates 18 U.S.C. § 1030(a)(6) if it "knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization." The term "traffic" means "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5). Plaintiffs allege that Defendants obtained Plaintiffs' and Class members' financial institution login credentials by posing as their financial institutions and then transferred access to Plaintiffs' financial accounts to their clients and partners. ¶ 230. The single case cited by Defendants is inapposite. MTD at 17. Unlike *Oracle Am., Inc. v. TERiX Computer Co., Inc.*, where plaintiffs "[did not allege] that Defendants transferred or otherwise disposed of its customer's login credentials," Plaintiffs here allege Defendants shared access to Plaintiffs' financial accounts with their app clients and partners. No. 5:13-cv-03385-PSG, 2014 WL 31344, at *6 (N.D. Cal. Jan 3, 2014).

F. Plaintiffs State a Claim for Violation of the California Anti-Phishing Act

The Anti-Phishing Act makes it "unlawful for any person, by means of a Web page, electronic mail message, *or otherwise through use of the Internet*, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2 (emphasis added). "Identifying information" includes a "[b]ank account number," "[a]ccount password," and "[a]ny other piece of information that can be used to access an individual's financial accounts." *Id.* § 22948.1(b).

Defendants do not dispute that they induced Plaintiffs to turn over their bank account credentials, or that those credentials are "identifying information." Instead, Defendants say there is no allegation that they disguised themselves as Class members' banks, MTD at 18, but this ignores extensive allegations in the Amended Complaint. *See, e.g.*, ¶ 6 ("[Class members] are prompted to enter their credentials into a log in screen that mirrors what they would see if they directly logged into their respective bank's website. Their financial institution's logo is

prominently displayed . . . ."), ¶ 45 ("[T]he customer believes that it is interacting with its home institution (e.g., its bank)."); ¶ 216 ("Defendants violated the Anti-Phishing Act by representing themselves to be . . . Class members' financial institutions.").[18]

Plaintiffs also plausibly allege that Defendants acted without authority or approval of financial institutions they imitate. ¶ 216. That allegation suffices at this stage of the litigation. The precise scope of Defendants' authority will be evident only from documents and information in Defendants' sole possession, such as bilateral contracts that Defendants have (or do not have) with those banks. Defendants should not obtain dismissal of the claim merely because discovery would be necessary to prove it. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1022 (9th Cir. 2018) ("[C]ontentions about the absence of certain facts . . . may be appropriate for summary judgment" but not "at the motion to dismiss stage.").

G. Plaintiffs State a Claim Under the UCL

1. Plaintiffs Properly Plead UCL Standing

There are "innumerable ways" that plaintiffs can show that they "suffered injury in fact and . . . lost money or property," for purposes of establishing UCL standing. *Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1019 (N.D. Cal. 2019). Some of those include by alleging that a plaintiff "surrenders in a transaction more, or acquires in a transaction less than he or she otherwise would have" ("benefit of the bargain"); has "a present or future property interest diminished"; or is "deprived of money or property to which he or she has a cognizable claim." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011); *see Ehret v. Uber Techs., Inc.*, 68 F. Supp. 3d 1121, 1134 (N.D. Cal. 2014) (economic injury sufficient to support UCL standing exists where plaintiff surrendered in a transaction more, or acquired less, than he or she otherwise would have). General allegations of injury suffice. *Gonzales*, 305 F. Supp. at 1093 (allegations that Uber accessed private communications satisfied the lost money or property requirement when combined with allegations that the conduct reduced drivers' earnings), *on recon.*, No. 17-CV-02264-JSC, 2018 WL 3068248 (N.D. Cal. June 21, 2018).

[18] It is simply false that Plaintiffs "knowingly provided their log-in credentials to Yodlee." MTD at 18. As discussed above, any purported consent was ineffective. *See supra* § III.E.2.

Plaintiffs allege that they lost money or property in at least four ways. *First*, they surrendered more to—and acquired less from—Defendants than they would have if they had known the truth about Defendants' data practices. *See In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) ("*Anthem I*") (allegations that Defendants did not adequately protect Plaintiffs' personal data as promised, thus causing benefit of bargain damages, suffice). *Second*, Plaintiffs allege that they would not have connected their bank accounts to the FinTech Apps via Yodlee if they had known the truth about Defendants' practices. ¶¶ 94, 189; *see Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1091 (S.D. Cal. 2016) (allegations that Plaintiffs would not have used a telephone system had they known the calls were being recorded sufficed). *Third*, Plaintiffs allege that they lost valuable indemnity rights that existed when Plaintiffs' private data was held at their banks alone. ¶¶ 92, 95, 97, 99. *See Gonzales*, 305 F. Supp. 3d at 1093; *Fraley v. Facebook, Inc*., 830 F. Supp. 2d 785, 810-12 (N.D. Cal. 2011) (holding that plaintiffs sufficiently alleged a loss of money or property based on potential compensation where Facebook used plaintiffs' Facebook profiles to endorse third party products and services). *Fourth*, Plaintiffs allege that Defendants' deceptive conduct caused them to lose control over valuable property and placed them at a heightened risk of identity theft and fraud. ¶¶ 95, 98, 99.

Defendants' argument that the alleged losses are purely "contingent losses that have not yet occurred" mischaracterizes the allegations in the Complaint. MTD at 19. Allegations that Plaintiffs lost valuable property rights or did not receive the benefit of the bargain describe harms they already suffered and convey UCL standing. *See Cappello*, 394 F. Supp. 3d at 1019-20.[19]

[19] Plaintiffs are entitled to plead alternative causes of action and seek duplicative or inconsistent remedies—including equitable and monetary relief—under Fed. R. Civ. P. 8(d). *See Astiana v. Hain Celestial Grp., Inc*., 783 F.3d 753, 762–63 (9th Cir. 2015); *Adkins v. Comcast Corp.*, No. 16-05969, 2017 WL 3491973, at *3 (N.D. Cal. Aug. 1, 2017) ("[There is] no basis in California or federal law for prohibiting the plaintiffs from pursuing their equitable claims in the alternative to legal remedies at the pleadings stage." (citation omitted)); *Luong v. Subaru of Am., Inc.*, No. 17-CV-03160-YGR, 2018 WL 2047646, at *7 (N.D. Cal. May 2, 2018) ("The availability of monetary damages does not preclude a claim for equitable relief under the UCL . . . based upon the same conduct.").

2. Plaintiffs Plead Each Element of a UCL Claim

"The UCL creates a cause of action for business practices that are: (1) unlawful, (2) unfair, or (3) fraudulent." *Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1145 (N.D. Cal. 2013) (internal quotation omitted) (emphasis added). "Each 'prong' of the UCL provides a separate and distinct theory of liability" that may support a cause of action." *Id.* Plaintiffs allege all three.

Unlawful: "Virtually any state, federal or local law can serve as the predicate for an action under section 17200." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 841 (N.D. Cal. 2020) (quoting *Davis v. HSBC Bank Nevada*, 691 F.3d 1152, 1168 (9th Cir. 2012)). Defendants' misuse of Plaintiffs' highly sensitive personal data violates California common law, the California Constitution, California Civil Code § 1709, and the SCA, among others. *See* ¶¶ 70-86, 142-82, 192-245. This satisfies the unlawful prong of the UCL.

Unfair: The UCL also creates a cause of action for business practices that are unfair "even if not specifically proscribed by some other law." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co*., 20 Cal. 4th 163, 180 (1999). Courts apply one of two tests to determine whether conduct against consumers is "unfair." *Davis*, 691 F.3d at 1169. First, unfair conduct violates the UCL if it violates public policy that is "tethered" to "some specific constitutional, statutory, or regulatory provisions." *Anthem I,* 162 F. Supp. 3d at 990 (conduct plausibly unfair where it violated "California's public policy of protecting consumer data"). Here, Defendants' covert collection of Plaintiffs' highly sensitive personal data violated California's public policy of protecting fundamental privacy rights, as enshrined in the California Constitution. ¶¶ 100-05. Second, Plaintiffs also satisfy the unfair prong by alleging conduct that: (a) was "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers" or "violates public policy," and (b) resulted in harm that outweighs its utility. *Anthem I*, 162 F. Supp. 3d at 990. Again, Defendants' conduct significantly harmed Plaintiffs without any countervailing benefit. ¶ 187.

Fraud: "To state a claim under the 'fraud' prong of [the UCL], a plaintiff must allege facts showing that members of the public are likely to be deceived by the alleged fraudulent business practice." *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL

3029783, at *34 (N.D. Cal. May 27, 2016) ("*Anthem II*"). Plaintiffs meet this requirement by alleging that Defendants' omission of key facts induced Plaintiffs to use Defendants' services, which they would not have done had they known the full scope of Defendants' practices. ¶¶ 94, 189. *See infra* § III.H.

H. Plaintiffs State a Claim Under California Civil Code § 1709

The elements of a claim for deceit under Cal. Civ. Code § 1709 are (a) misrepresentation or omission, (b) knowledge of falsity; (c) intent to defraud; (d) reliance; and (e) damage. *Chassin Holdings Corp. v. Formula VC Ltd.*, No. 15-CV-02294-EMC, 2017 WL 66873, at *8 (N.D. Cal. Jan. 6, 2017). While all fraud claims are subject to Rule 9(b)'s pleading standard, allegations of omission-based fraud may be less specific. *See supra* § III.A.

1. Duty to Disclose Material Facts

A defendant's omission is actionable where it had a duty to disclose. *Duttweiler v. Triumph Motorcycles (Am.) Ltd.*, No. 14-CV-04809-HSG, 2015 WL 4941780, at *4 (N.D. Cal. Aug. 19, 2015) (citing *Daugherty v. Am. Honda Motor Co*., 144 Cal. App. 4th 824, 835 (2006)). California imposes such a duty if "the defendant actively conceals a material fact from the plaintiff," "the defendant had exclusive knowledge of material facts not known to the plaintiff" or "the defendant makes partial representations but also suppresses some material facts." *Terpin v. AT&T Mobility, LLC*, No. 2:18-cv-06975 (ODW) (KSX), 2020 WL 5369410, at *3 (C.D. Cal. Sept. 8, 2020) (internal citations omitted). Here, Defendants had a duty to disclose to Plaintiffs the full scope of their data practices because they: (1) actively concealed those practices, ¶ 59; (2) maintained exclusive knowledge about material facts not known to Plaintiffs, ¶¶ 54-69, 177-78; and (3) made partial representations regarding those suppressed material facts, ¶¶ 56, 59-60.

2. Knowledge of Falsity and Intent to Defraud

Plaintiffs allege that Defendants knowingly misled Plaintiffs and intentionally harvested their data. Plaintiffs need only allege this element generally. *See supra* § III.A; Fed. R. Civ. P. 9(b). The Amended Complaint is replete with allegations that "Defendants intentionally engaged in the misconduct alleged herein for their own financial benefit unrelated to any service they provide." ¶ 148.

3. Plaintiffs Allege that They Would Have Acted Differently Had They Known the Truth About Defendants' Data Practices

To satisfy the reliance prong based on a material omission, a plaintiff need only allege that "had the omitted information been disclosed, the plaintiff would have been aware of it and behaved differently." *Anthem II*, 2016 WL 3029783, at *35.

Plaintiffs allege that had they "known the true nature, significance and extent of Defendants' data practices, they would not have used Yodlee." ¶¶ 94. The fact that Plaintiffs have not "de-linked their PayPal account[s]" does not undermine their claim. MTD at 22. The reliance requirement tests whether "the misrepresentation or nondisclosure was an *immediate cause* of the plaintiff's conduct" at the time they "entered into the contract or other transaction." *City Solutions, Inc. v. Clear Channel Communications*, 365 F.3d 835, 840 (9th Cir. 2004) (emphasis added) (quoting *Alliance Mortgage Co. v. Rothwell*, 900 P. 2d 601, 609 (1995)). What Plaintiffs would do *now* given the same information is irrelevant.

4. Plaintiffs Properly Plead Damages

Plaintiffs sufficiently allege damages for the same reasons discussed above. *See, e.g.*, *supra* § III.E.4. Defendants citation to *Ha v. Bank of America* is inapposite. MTD at 22 (citing *Ha v. Bank of America*, No. 5:14-CV-00120-PSG, 2014 WL 6904567, at *2 (N.D. Cal. Dec. 8, 2014)). The *Ha* court dismissed plaintiff's claims, finding their causation allegations to be "speculative" where plaintiff's own failure to make timely mortgage payments provided an independent cause of harm. *Id* at *3. That reasoning does not apply here because Defendants' conduct—not Plaintiffs'—directly caused Plaintiffs' injuries.

I. Plaintiffs State a Claim for Unjust Enrichment

"California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." *Facebook Tracking*, 956 F.3d at 599 (plaintiffs' allegations sufficed for standing purposes), 611 (plaintiffs stated a claim); *Facebook Consumer Privacy*, 402 F. Supp. 3d at 803 ("[E]ven if the

plaintiffs suffered no economic loss from the disclosure of their information, they may proceed at this stage on a claim for unjust enrichment to recover the gains that Facebook realized from its allegedly improper conduct.").

Here, Plaintiffs allege that Defendants were unjustly enriched by acquiring Plaintiffs' sensitive financial data through a fraudulent scheme and then selling subscriptions to that data for millions of dollars a year to their "analytics and insights" customers. ¶ 11. There is no merit to Defendants' argument that Plaintiffs have not identified the misleading statements. ¶¶ 54-60.[20] Plaintiffs have a right to recover the gains that Defendants realized from their allegedly improper conduct, and their cause of action for unjust enrichment is the proper means of doing so.

IV. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court deny Yodlee's motion to dismiss.

DATED: December 16, 2020

/s/ Aaron M. Sheanin

Aaron M. Sheanin (SBN 214472)
Christine S. Yun Sauer (SBN 314307)
ROBINS KAPLAN LLP
46 Shattuck Square, Suite 22
Berkeley, CA 94040
Telephone: (650) 784-4040
Facsimile: (650) 784-4041
ASheanin@RobinsKaplan.com
CYunSauer@RobinsKaplan.com

Kellie Lerner (*pro hac vice* forthcoming)
David Rochelson (admitted *pro hac vice*)
ROBINS KAPLAN LLP
399 Park Avenue, Suite 3600
New York, NY 10022
Telephone: (212) 980-7400
Facsimile: (212) 980-7499
klerner@robinskaplan.com
drochelson@robinskaplan.com

[20] As explained above in footnote 19, Plaintiffs may plead alternative causes of action and seek duplicative or inconsistent remedies under Fed. R. Civ. P. 8(d). Therefore, Defendants' contention that Plaintiffs may not assert an unjust enrichment claim fails. Plaintiffs agree to withdraw their claim under the Declaratory Judgment Act.

Thomas J. Undlin (*pro hac vice* forthcoming)
ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402
Telephone: (612) 349-8500
Facsimile: (612) 339-4181
tundlin@robinskaplan.com

Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Facsimile: (914) 997-0035
achristina@lowey.com

John Emerson (*pro hac vice* forthcoming)
EMERSON FIRM, PLLC
2500 Wilcrest Drive
Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659
jemerson@emersonfirm.com

Robert Kitchenoff (*pro hac vice* forthcoming)
WEINSTEIN KITCHENOFF & ASHER LLC
150 Monument Road, Suite 107
Bala Cynwyd, PA 19004
Telephone: (215) 545-7200
kitchenoff@wka-law.com

Adam Frankel (*pro hac vice* forthcoming)
GREENWICH LEGAL ASSOCIATES LLC
881 Lake Avenue
Greenwich, CT 06831
Telephone: (203) 622-6001
afrankel@grwlegal.com

Attorneys for Plaintiffs and the Proposed Classes